**MILITARY HEALTH SYSTEM (MHS)**

**INFORMATION ASSURANCE (IA)**
**IMPLEMENTATION GUIDE**

| | | |
|---|---|---|
| **IMPLEMENTATION GUIDE No. 12** | | |
| **EFFECTIVE DATE**<br>07/19/05 | **REVISED DATE**<br>xx/xx/xx | |

**Subject:**

**INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) PROGRAM**

## 1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TMA Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

The Information Assurance Vulnerability Alert (IAVA) process (instituted in 1998) provides positive control of vulnerability notification and corresponding corrective action for DoD network assets. The Information Assurance Vulnerability Management (IAVM) Program supersedes the previous IAVA process. Vulnerabilities in computing systems and networks are weaknesses that could compromise sensitive or patient health information and deny service to beneficiaries of the MHS.

The IAVM program notifies Combatant Commands, Services, and Agencies (CC/S/A) about vulnerability alerts and mitigation measures. The DoD-Computer Emergency Response Team (CERT) is responsible for the dissemination of vulnerability information to CC/S/A points of contact (POCs). Joint Task Force Global Network Operations (JTF GNO) provides notification of IAVAs, Information Assurance Vulnerability Bulletins (IAVBs), and Information Assurance (IA) Technical Advisories (TAs) to the MHS. These notices include information about the mitigation of vulnerabilities, malicious code, and other threats to the DoD.

# 2 POLICY

It is MHS policy that TMA Components shall monitor and report mitigation of known IAVAs to the MHS IAVM Monitor through the DoD Vulnerability Management System (VMS). U.S.

The DoD MHS IAVM guidance establishes an IAVM program that provides responsive and effective vulnerability management as required by Chairman of the Joint Chief of Staff Manual (CJCSM) 6510.01, "Computer Network Defense." This implementation guide establishes responsibilities and procedures for IAVM programs, to include organizational and individual responsibilities, registration, compliance criteria, extensions, enforcement, and verification.

# 3 PROCEDURES

3.1 Each Program identified within the TMA Components shall:

a. Designate a primary and secondary representative responsible for managing its internal IAVM program and register primary and secondary POCs in the VMS.

b. Acknowledge receipt of the IAVA or IAVB messages within five days of release.

c. Disseminate vulnerability messages via command channels to all appropriate organizations within the MHS, to include but not limited to program managers, Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), System Administrators (SAs), and/or other personnel responsible for implementing and managing responses to IS vulnerabilities.

d. Ensure all subordinate organizations comply with all IAVAs within the designated compliance window or in accordance with the extension process.

e. Report IAVA compliance status via VMS as specified in the individual IAVA message (typically 30 days from the date on the message) and update the VMS weekly, at a minimum.

f. Review second and third extensions and their associated mitigation plans and implementation timelines. This role will be filled by the appropriate Designated Approving Authority (DAA) for the organization.

g. Establish a process to ensure that all DoD contracts for DoD ISs and services contain language requiring participation in the IAVM program.

h. Conduct IAVM program compliance checks of their subordinate organizations.

3.2 Roles & Responsibilities

3.2.1 The DAA shall:

a. Order the affected assets disconnected from the network if unable to submit an action plan describing steps to be taken to achieve compliance with outstanding IAVAs.

b. Review extension requests and, if appropriate, disconnect compromised systems from the network immediately.

c. Review and, if appropriate, approve the first 30-day extension (local DAA) that would allow continued operation of the non-compliant system. DAA-authorized extensions shall not exceed the period of the first extension without TMA review and approval.

3.2.2 The IAM shall:

a. Ensure IAVA notices are disseminated to the lowest level IAOs, SAs, and other individuals identified as participants in the IAVM process.

b. Ensure all subordinate organizations comply with all IAVAs within designated compliance window or in accordance with the extension process.

c. Monitor IAVBs and TAs.

d. Review requests for extensions; monitor extension plans with their associated mitigation plans and implementation timelines as required.

e. Ensure that all required risk mitigation actions are implemented in accordance with associated timeline if extension to an IAVA is granted.

f. Ensure compliance checks of their subordinate organizations to make certain mitigating and/or corrective actions are completed.

g. Review approved mitigation action plan and include it as part of an extension request.

3.2.3 Programs centrally managed at the TMA level or at the MHS Enterprise level must establish a capability to effectively mitigate the risk posed by critical vulnerabilities as identified in IAVA notices. Joint or Enterprise-wide Program Managers shall:

a. Register with the VMS for a User Identification (ID) and password for VMS.

b. Designate a primary and secondary IAVM POC.

c. Respond to each IAVM message as the system configuration manager.

d. Acknowledge receipt of the IAVM messages through VMS.

e. Publish a program action plan for every IAVM notice issued by DoD CERT; the program plan should provide an initial status.

f. Provide periodic status updates, as required, throughout the life cycle of the vulnerability until the corrective action has been completed.

g. Ensure dissemination of the action plan, if necessary, to affected SAs.

h. Process program level extensions through the appropriate program DAA.

3.2.4 The IAO shall:

a. Maintain positive configuration control of all ISs and/or assets under their purview. Maintain configuration documentation that identifies specific system and/or asset owners and SAs including applicable network addresses.

b. Ensure networked assets are managed and administered in a manner allowing both chain of command and authorized independent verification of corrective actions.

3.2.5 Designated IAVM representatives shall:

a. Register with the MHS IAVM Monitor for assignment of User ID and password in the VMS system.

b. Disseminate IAVA notices to lowest level SAs.

c. Enter their organization's acknowledgment and compliance and/or extension data into VMS/Vulnerability Compliance Tracking System (VMS/VCTS).

d. Monitor compliance status for IAVM Alerts, and update VMS as statistics change throughout the life cycle of the IAVA.

e. Prepare, review, and forward requests for extensions. Extensions should be passed along to the DAA for further review and adjudication.

3.2.6 The SA shall:

a. Ensure all devices are IAVA compliant prior to connecting the devices to DoD networks.

b. Respond to all active IAVAs – any asset found with an active vulnerability, where the IAVA completion date has closed, must be brought into compliance immediately, have an extension request submitted, or the asset must be disconnected.

c. Test and evaluate all patches intended to resolve an IAVA and obtain permission from the Project Officer before deploying the fix to a device. An extension should be requested if the supplied fix is unsatisfactory and another fix must be researched or developed.

d. Monitor for new vulnerability notices.

e. Report compliance and/or extension information through the command channels for aggregation and reporting.

f. Prepare and submit an extension and mitigation action plan (including implementation timelines) within the time specified in the IAVA notification message (usually 30 days), if unable to comply with an IAVA.

g. For centrally managed systems, test and evaluation of IAVA will be performed by JMISO. JMISO will identify when IAVA are approved for deployment.

## 3.3 IAVA Extensions and Compliance Process and Timelines

3.3.1 The extension process has been broken into three categories (First, Second, and Third extensions).

- The FIRST extension begins the day after the original compliance window identified in the IAVA notification message closes and runs for up to 30 days (Note: The normal compliance window is 30 days, but may be adjusted by the JTF GNO).
- The SECOND extension begins the day after the first extension ends and runs for 60 days.
- The THIRD extension begins the day after the second extension ends and runs for a period directed by the approval authority, for a maximum of two years.

3.3.2 Extension approval authority is determined by the extension category being requested. Once extensions are approved, VMS must be updated to reflect the approval. The database must also be updated when the extension has been closed.

3.3.3 First extensions are approved by the local DAA. Approval of this first extension authorizes the system to operate for 30 additional days while mitigation actions are implemented to reduce risk. Extension requests must include:

a. System being addressed.

b. Name of system.

c. Description of system, including media access control (short paragraph).

d. Internet Protocol address and machine name (if applicable).

e. Media access control address (if applicable).

f. IAVA number.

g. Date of the request.

h. Estimated date of completion.

i. Reason for extension.

j. A plan of action (POA) describing in detail what steps will be taken to test and apply an appropriate patch for the vulnerability described within the IAVA.

k. A series of milestones indicated within the POA that provide a specific timeline for remedy actions.

l. A risk assessment of high, medium, or low risk. Risk assessment should consider, as a minimum, the number of systems affected, indications and warnings, mitigation plans and/or actions, and potential operational impact of non-compliance).

m. Identification of the approving DAA.

n. POC (Name, e-mail address, telephone number).

Approval must be based on a sound extension plan with mitigation actions that minimize the risk of compromise to local systems. Local DAAs must consider the associated risk shared by other DoD networks when approving an extension.

3.3.4 The TMA Component DAA approves second extensions. Approval of this second extension allows the asset to operate for 60 additional days while mitigating activities are performed.

a. Any additional mitigation actions required to protect assets during the second extension period must be provided along with a strong justification for extension.

b. The MHS Chief Information Officer (CIO) approves third extensions. Third extensions are reserved for rare cases where circumstances have prevented compliance with an IAVA during the timelines for first or second extension, to include mission required legacy systems that cannot meet IAVA requirements. The extension packages must be revalidated, including the latest extension plan, timeline, and proposed mitigation actions.

3.3.5 Third extension mitigation plan shall include:

a. Mitigating policies, processes, and procedures that have been implemented (e.g., actions that have been prohibited or controlled or monitoring processes that have been employed or intensified).

b. Network-level actions, to include use of security tools such as firewalls, security routers, proxy devices, and intrusion detection systems (IDSs).

c. Server-level actions to limit attachment size on exchange servers.

d. Any system-level actions, such as disabling services, host level firewalls, and IDSs, as necessary.

e. A statement that a vulnerability assessment, evaluating the effectiveness of the mitigating actions, has been conducted of the vulnerable system; a copy of vulnerability assessment must be available for review.

f. A statement of milestones and end date for accomplishing the IAVA implementation.

Open third extensions shall be reviewed and revalidated by the MHS CIO at least annually, and VMS shall be updated to reflect the outcome of the review. The database must be updated when the extension has been closed. USSTRATCOM shall monitor third extensions and updates for potential risk to Defense Information Systems Network (DISN). USSTRATCOM may request additional information from the MHS CIO authorizing the third extension. USSTRATCOM may request a review (by exception) of extensions by DISN DAAs in cases of potential unacceptable risk to DISN or when extension documentation problems could not be resolved. This request for review by DISN DAAs shall be sent through Joint Staff, J-6K.

The Joint Staff shall notify the MHS CIO and request that USSTRATCOM conduct a risk assessment of extension continuation for the DISN DAAs. This risk assessment shall be conducted in coordination with USSTRATCOM, Defense Information Systems Agency (DISA), the National Security Agency (NSA) and the CC/S/As requesting the extension. Recommendations shall be made to the DISN Security Accreditation Working Group (DSAWG).

The DSAWG shall review recommendations and shall approve extension continuations (as delegated to them by DISN DAAs). The DSAWG may also request additional information or provide further guidance for extension continuation. The MHS CIO may appeal DSAWG guidance to the DISN Flag Panel. Acting as the direct representatives of the DISN DAAs, the Flag Panel shall adjudicate all requests forwarded from the DSAWG. If the Flag Panel determines that a request is of such a critical nature that it requires the DISN DAAs to decide, it shall be forwarded with a Flag Panel recommendation.

Systems covered by third extensions requests are subject to independent vulnerability analysis as directed by the extension approving authority.

### 3.4 VMS User Enrollment and Training

All users assigned responsibility to update or monitor IAVM compliance in VMS shall apply for and obtain a VMS account. The MHS IAVM Coordinator shall create VMS accounts and assign appropriate permissions, or allow heads of Program Offices to assign permissions to their subordinate users.

Individuals who wish to apply for an account within VMS should complete a DD Form 2875, “System Authorization Access Request (SAAR)”, May 2004, available from DISA, and return the completed form to the MHS IAVM Coordinator for review and approval by MHS IA or JMIS, as appropriate. Applicants should contact the MHS IAVM Coordinator to obtain guidance on how to properly complete the DD Form 2875 before submitting their form.

Applicants should meet the minimum qualifications prior to applying for a VMS account:

- For United States (U.S.) citizens: Possess a NAC or better investigation, and accompanying interim or final investigation or designation.
- For non-U.S. citizens: Possess a final Secret or Top Secret clearance, or a final ADP/IT-I, II, or III designation.

Training is available through DISA and within the VMS application. New VMS users should review the training module available within the VMS application, or contact DISA for live training.

Interim Access: Upon completion and submission of appropriate paperwork, interim access may be granted. Interim access is granted only to US citizens.

3.5 Component Non-Compliance Notification and Enforcement Procedures

a. Commander, USSTRATCOM, shall notify noncompliant DoD component IAVA authority POC to verify IS or network is non-compliant and to coordinate a resolution.

b. DoD components shall be considered non-compliant under any of the following conditions:

   - DoD organization has not acted to update IAVA status within directed compliance window.
   - Non-compliant computer assets operating without approved extension and mitigation plan.

     If TMA is not responsive or fails to follow through with resolving the non-compliance, USSTRATCOM shall release an IAVA noncompliance message addressed to the TMA director.

c. Non-compliant DoD components shall be requested to respond within 72 hours with reasons for non-compliance, planned corrective actions, mitigation plan, and operational impact; DoD components shall respond to USSTRATCOM.

d. USSTRATCOM shall review planned component corrective actions and coordinate any additional actions required to mitigate vulnerability created by non-compliance in accordance with Paragraph 5.12.5, DoD Directive O-8530.1, “Computer Network Defense”, January 8, 2001.

   - USSTRATCOM, in coordination with the Joint Staff (J-3 and J-6), shall determine global operational impact of continued IAVA noncompliance as required.

- If USSTRATCOM or a DoD component has an issue that cannot be resolved concerning compliance actions, Assistant Secretary of Defense (Networks & Information Integration) (ASD(NII)) and the Chairman of the Joint Chiefs of Staff shall be informed.

## 4 REFERENCES

a. DoDD 8500.1, “Information Assurance (IA),” October 24, 2002

b. DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003

c. CJCSM 6510.01, Change 1, “Defense in Depth: Information Assurance and Computer Network Defense,” August 10, 2004

d. DoDI 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997

e. DoDI O-85301, “Computer Network Defense”, January 8, 2001.

f. DoDI O-8530.2, “Support to Computer Network Defense (CND),” March 9, 2001

g. DoD 5200.1-R, “Information Security Program,” January 1997

h. DoD 5200.2-R, Change 3, “Personnel Security Program,” February 23, 1996

i. Federal Information Security Management Act of 2002

j. Health Insurance Portability and Accountability Act (HIPAA) Security Final Rule, February 20, 2003.

## 5 ACRONYMS

| | |
|---|---|
| ADP | Automated Data Processing |
| ASD(NII) | Assistant Secretary of Defense (Networks & Information Integration) |
| CC/S/A | Combatant Commands, Services, and Agencies |
| CERT | Computer Emergency Response Team |
| CIO | Chief Information Officer |
| CJCSI | Chairman of the Joint Chiefs of Staff Instruction |
| CJCSM | Chairman of the Joint Chiefs of Staff Manual |
| CND | Computer Network Defense |
| DAA | Designated Approving Authority |
| DISA | Defense Information Systems Agency |
| DISN | Defense Information Systems Network |
| DoD | Department of Defense |
| DoDD | Department of Defense Directive |
| DoDI | Department of Defense Instruction |

| | |
|---|---|
| DSAWG | Defense Information Systems Network (DISN) Security Accreditation Working Group |
| IA | Information Assurance |
| IAM | Information Assurance Manager |
| IAO | Information Assurance Officer |
| IAVA | Information Assurance Vulnerability Alert |
| IAVB | Information Assurance Vulnerability Bulletin |
| IAVM | Information Assurance Vulnerability Management |
| ID | Identification |
| IDS | Intrusion Detection System |
| IS | Information System |
| IT | Information Technology |
| JMISO | Joint Medical Information Systems Office |
| JTF-GNO | Joint Task Force, Global Network Operations |
| MHS | Military Health System |
| NSA | National Security Agency |
| PEO | Program Executive Office |
| POA | Plan of Action |
| POC | Point of Contact |
| SA | System Administrator |
| TA | Technical Advisory |
| TMA | TRICARE Management System |
| TRO | TRICARE Regional Offices |
| USSTRATCOM | United States Strategic Command |
| VCTS | Vulnerability Compliance Tracking System |
| VMS | Vulnerability Management System |